IN THE UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

IN RE: GERBER PRODUCTS COMPANY HEAVY METALS BABY FOOD LITIGATION	Master File No. 1:21-cv-00269 (MSN/JFA)
This Document Relates to ALL Cases	

STIPULATION AND ORDER REGARDING DISCOVERY OF ELECTRONICALLY STORED INFORMATION

Plaintiffs and Defendant Gerber Products Company ("Parties") hereby agree and stipulate as follows:

1. **Purpose**: This Stipulation and Order will govern discovery of electronically stored information ("ESI") in this case as a supplement to the Federal Rules of Civil Procedure, this Court's Guidelines for the Discovery of Electronically Stored Information, and any other applicable orders and rules.

2. **Search**: The parties will meet and confer about methods to search ESI in order to identify relevant ESI that is subject to production in discovery including the process for negotiating electronic search methodologies and the disclosures necessary for such negotiations, as well as the validation of such methodologies. As part of the meet and confer the parties will agree to a list of preliminary search terms. Within 5 days of its creation, the responding party will share the "hit report" generated by the preliminary search terms. The parties will meet and confer on adding, removing, or modifying terms.

3. **File Exchange for Use in Transmitting Productions.**

a. All data should be encrypted when transferred. Secure FTP with a password protected ZIP file or Encrypted Padlock Hard Drive/Flash Drives should be provided for all productions.

b. ZIP file passwords should be provided in a separate email or under separate cover.

4. **Document Depositories**

After a meet and confer, the parties agreed that each party shall bear its own costs to store and review data (including to retain an eDiscovery vendor to facilitate the hosting, review, examination, and production of documents, as each party deems appropriate). In the event that the receiving party has difficulty processing or accessing documents transmitted by the producing party, the receiving party shall meet and confer with the producing party to facilitate prompt and efficient resolution.

5. **Information Security Program**. Any person in possession of documents or information designated "Confidential," "Highly Confidential," or other similar designation pursuant to the Stipulation and Protective Order entered by the Court in this action shall maintain an information security program that includes reasonable administrative, technical, and physical safeguards designed to protect the security and confidentiality of such documents and information, protect against any reasonably anticipated threats or hazards to the security of such documents and information, and protect against unauthorized access to such documents and information, in the same manner as it would for its own such documents and information. If a receiving party or authorized recipient discovers any loss of such documents or information or a breach of security, including any actual or suspected unauthorized access, the receiving party or authorized recipient

shall: (1) promptly provide written notice to the disclosing party of such breach; (2) investigate and make reasonable efforts to remediate the effects of the breach, and provide the disclosing party with assurances reasonably satisfactory to the disclosing party that such breach shall not recur; and (3) provide sufficient information about the breach that the disclosing party can reasonably ascertain the size and scope of the breach. The receiving party agrees to cooperate with the disclosing party and/or law enforcement in investigating any such security incident. In any event, the receiving party shall promptly take all necessary and appropriate corrective action to terminate the unauthorized access.

6. **Deduplication.** The producing party is only required to produce a single copy of a responsive document (*i.e.*, TIFF or PDF) and may de-duplicate responsive ESI (based on MD5 or SHA-1 hash values at the document level) globally and across custodians. For emails with attachments, the hash value is generated based on the parent/child document grouping. However, metadata identifying all custodians in possession of each document that is removed as a duplicate must be produced, to the extent it exists at the point of collection, or is created through the deduplication process, in an "ALL CUSTODIAN" field in the production load file.

7. **Document Identifier.** Each produced document must have a unique and sequential Bates number added to the lower right-hand corner of the page, and any confidential designation added to the lower left-hand corner. The Bates number and/or designation should not interfere with the information presented in the document.

8. **Load Files.**

a. .DAT file – A .DAT file with standard Concordance delimiters for loading metadata, text, and native files into Relativity should be produced.

b. .OPT – A standard Opticon .OPT load file to link all image paths and documents breaks should be produced.

9. **Images.** Images should generally be provided as Black & White, Single Page, Group IV, 1-Bit TIFF files. However, if producing a document in black and white that was originally in color alters or obscures the substance of the document, then, upon reasonable request, the document will be produced in color as single-page 300 DPI JPG images, to the extent possible.

10. **Extracted Text/OCR Files.**

a. All documents produced should have a corresponding document level text file. The path to the text file should be included in the .DAT file in the OCR Text field.

b. The name of the document level text files should reflect its corresponding production number (e.g., CTRL00000001.txt, CTRL00000002.txt).

11. **Embedded Files.** Except as provided below, embedded files are to be fully extracted, and the appropriate parent-child relationship must be maintained unless such original document is produced in native format with the embedded information contained within it. Examples of embedded files include but are not limited to the following:

a. ZIP files and other compressed file formats;

b. Embedded PDF file formats;

c. Embedded e-mails that exist as an attachment to an e-mail.

The producing party need not produce embedded files as separate files that do not have user created content, including but not limited to irrelevant inline image files (*e.g.*, logos, icons, emoticons, and footers). The producing party need not produce embedded Excel files as separate files that have only duplicative data and do not hit search terms included in the parent document

from which they were extracted. The requesting party can meet and confer with the producing party to request the underlying Excel files.

12. **Email Families.** All parent/child document relationships must be maintained unless otherwise agreed upon. These fields should be identified in the PRODBEGATTACH or Group Identifier field contained in the .DAT file. When an attachment is withheld for privilege, the producing party shall produce a one-page TIFF image (or PDF if production format dictates) in place of the withheld attachment, correspondingly stating "Attachment Withheld--Privileged," and bearing a sequential BATES number within the family BATES range.

13. **Metadata.** Each of the metadata and coding fields set forth in Appendix A that can be extracted shall be produced for that document. The producing party is not obligated to manually populate any of the fields in Appendix A if such fields cannot be extracted from a document, with the exception of the following: PRODBEGBATES, PRODENDBATES, PRODBEGATTACH, PRODENDATTACH, ALL CUSTODIANS, CONFIDENTIALITY, PAGE COUNT, and REDACTED. The producing party shall make reasonable efforts to ensure metadata fields automatically extracted from the documents are correct.

14. **Documents Produced in Native Format.** Native files shall be produced for the following data types below with a corresponding TIFF placeholder. The name of the native file should reflect its corresponding Bates number (e.g., CTRL00000001.xlsx, CTRL00000002.wav).

a. Audio files (.mp3, .wav, .ram, .ra, .mid, etc.)

b. Video files (.3g2 .3gp .asf, .asx, .avi, .flv, .mov, .mp4, .mpg, .rm, .swf, .vob, .wmv, etc.)

c. Microsoft Excel documents and CSV files

i. The Microsoft Excel document or CSV file should be produced in the same format as collected except as outlined in subsection c.ii. below.

ii. If a Microsoft Excel document or CSV file requires redaction, then TIFF images of the document after the redaction has been applied shall be provided and the native file and full text may be withheld or a party may redact native Excel files by inserting "redacted" where the material is redacted if the producing party maintains a pristine non-redacted version of the Excel. The produced file should be named for the starting production number and the confidentiality designation.

d. If necessary, the parties will meet and confer regarding production of other file types in native format.

15. **Image Placeholders.** For documents produced natively or withheld from responsive families, image placeholders should be produced and include a text description of the reason for withholding (*i.e.* "DOCUMENT PRODUCED NATIVELY") and should be branded with a corresponding Bates number and any confidentiality designation required.

16. **Microsoft Office, WordPerfect, and Other Standard Documents (e.g., Google Docs and PDF Documents).** MS Office files, WordPerfect, and other standard documents, such as PDF documents and the like, shall be converted to single-page TIFF and produced consistent with the specifications herein. If the document contains comments or tracked changes, the TIFF images shall be generated to include the comments or tracked changes contained in the file.

17. **Microsoft PowerPoint and Other Presentation Files.** The parties will produce slide shows (e.g. Microsoft PowerPoint presentations) not requiring redaction in native format. Slide shows requiring redaction will be produced as TIFF images with corresponding searchable

OCR text (or in searchable PDF if production format dictates) and the associated metadata for the document, ensuring the redacted content is fully protected from disclosure.

18. **Production of Databases and Other Structured Data**. Production of responsive data contained in an enterprise database should be achieved via report or export of such data to MS-Excel spreadsheets or .csv files that will be produced, if reasonably feasible. If this is not reasonably feasible, the parties will meet and confer regarding a reasonable format. The requesting party may make reasonable requests for additional information to explain the database schema, codes, abbreviations, and different report formats or to request specific data from identified fields.

19. **Redactions.** In the event a document requires redaction, native files, full text and/or OCR, and specified metadata fields may be excluded. Metadata fields for exclusion in redacted documents include EMAIL SUBJECT, ORIGINAL FILENAME, and ORIGINAL FILEPATH, unless those fields contain information that should be withheld in line with the redactions performed. The TIFF or PDF image should use a black solid line or some other marking to show the word is clearly viewed as a redaction (*e.g.*, a label with the word "redacted") where applicable and the REDACTED field should be populated "Yes" to indicate the document contains a redaction. The reasoning for the redaction should be populated within the redaction text on the face of the document (*e.g.*, REDACTED – AC PRIVILEGE) or within a metadata field. In addition to redactions for any asserted privilege or other protection, the parties may use redactions to protect information prohibited from disclosure by federal, state, or foreign statutes or regulations, non-responsive medical information concerning any individual person, non-responsive personally identifiable information or sensitive personal information, and non-responsive commercially sensitive information not needed to understand the context of the responsive material.

20. **Password Protected Files.** The producing party shall make reasonable efforts to identify any potentially relevant ESI that is password protected or encrypted and undertake to remove those passwords or decrypt any encryption in order for the documents to be searched and/or reviewed. If the producing party's efforts are unsuccessful, it shall identify the file(s) at issue and meet and confer with the receiving party to discuss next steps, if any.

21. **Hard Copy Documents.**

a. Hard copy documents shall be scanned and produced in electronic form by converting them to single-page PDF or TIFF images and producing them following the same protocol set forth herein.

b. Images of all file labels, file headings, and file folders associated with any hard copy document shall be produced with the images of the hard copy documents.

c. Document breaks for paper documents should be captured by physical boundaries (clips, folders, staples, etc.). There is no obligation for a party to unitize paper documents unless it does so for its own review, and in that case, it should be replicated for production.

d. The database load file shall include the following fields: PRODBEGBATES, PRODENDBATES, PRODBEGATTACH, PRODENDATTACH, CUSTODIAN, CONFIDENTIALITY, and REDACTED.

22. **Phasing**. The parties will endeavor to produce responsive ESI on a rolling basis. The parties agree to meet and confer to consider prioritizing the production of (i) documents responsive to certain custodians identified in the parties' Initial Disclosures; and (ii) categories of non-custodial responsive documents. If either party feels production has been unreasonably

delayed, the parties agree to promptly confer via telephone or in person to reach a mutually agreeable consensus prior to court involvement.

23. **Privilege Log**. Within 21 days of the production of documents from which privileged documents are withheld, the producing party will produce a privilege log in Microsoft Excel format.

a. **Privilege Log Contents**. Communications with outside/litigation counsel do not need to be included in any privilege log. Every privilege log should (a) identify which listed individuals are attorneys; and (b) contain the following fields for each document entry, to the extent that they are available:

i. A unique privilege log identifier associated with each privilege log record, or the Bates number of a redacted Document, or the Bates number of a Document withheld but for which a placeholder TIFF was produced;

ii. Custodian;

iii. AllCustodian (if applicable);

iv. FileName;

v. EmailSubject (unless the subject/title itself contains privileged information in which case a reasonably objective "substitute" subject/title will be provided in a manner that, without revealing information itself privileged or protected, will enable other Parties to assess the claim. It must be clearly indicated that this is a "substitute" subject/title.);

vi. Author;

vii. From;

viii. To;

ix. CC;

x. BCC;

xi. DateSent;

xii. DateReceived;

xiii. DateCreated;

xiv. DateLastModified; and

xv. the nature of the privilege asserted ("ACP" and/or "WP").

In addition to these fields, the producing party must also include a field on its privilege log entitled "Attorney/Description of Privileged Material" with a description of the contents of the Document sufficiently detailed for the requesting party or the Court to evaluate the claim of privilege and determine which document or documents in a document family (i.e., email attaching memorandum) contain privileged material.

b. **Protocols for Logging Email Chains**. Any email chain (i.e., a series of emails linked together by email response and forwarding) that is withheld or redacted on the grounds of privilege, immunity, or any similar claim shall be logged as one Document and shall be identified by the top-most email in the chain that is withheld or redacted subject to the extent that there is more than one branch of (i.e., more than one unique group of recipients of) an email thread, each branch will be individually logged. The parties shall not be required to log identical copies of an email that is included in a chain that has been logged in accordance with this Paragraph.

c. **Protocol for Logging "Families."** Where an entire family is withheld, a single log entry for the family is permitted.

d. **Protocol for Challenging Privilege Logs**. Following the receipt of a privilege log, a requesting party may identify, in writing (by Bates/unique identification number),

the particular documents that it believes require further explanation. The producing Party shall endeavor to respond to such a request within 10 days. If a Party challenges a request for further information, the Parties shall meet and confer to try to reach a mutually agreeable solution. If they cannot agree, the matter may be brought to the Court.

e. Notwithstanding any of the foregoing, all parties reserve the right to seek to log some or all privileged documents by category, rather than "document-by-document," at a later date and after the volume and nature of any privileged documents is known.

24. **Use of Image Copy**. When documents produced in accordance with this protocol are used in any proceeding herein, including depositions, hearings, or trial, the image copy of documents as described herein shall be the copy used unless the document was produced in native or the image copy is so illegible or unwieldy to make it infeasible to use as a deposition exhibit, in which case the native version may be used. If the native version is used as an exhibit, the record of the deposition must identify the exhibit using its BATES number, and the BATES number shall also be written on any paper or electronic copy of the exhibit. The document shall not be modified for use without the consent of the producing party. The confidentiality designation of the document shall also be stated on the record of the deposition and shall be written on any paper or electronic copy of the exhibit. Extracted text files shall not be used in any proceeding as a substitute for the image of any document. This paragraph does not apply to any summary exhibits or demonstratives.

25. **Costs**. Each party will bear the costs to process and review its own documents according to this protocol. Notwithstanding this paragraph, nothing in this protocol limits or prohibits a prevailing party from seeking recovery of all allowable fees and costs, including attorney fees and costs, as may be permitted under applicable law.

26. **Protective Order**. Nothing in this protocol shall be construed to affect, modify, or amend any protective order the parties file with the Court.

27. **Discoverability and Admissibility**. Nothing in this protocol shall be construed to affect the discoverability or admissibility of any document or data. All objections to the discoverability or admissibility of any document or data are preserved and may be asserted at any time in accordance with the applicable rules.

28. **No Waiver.** The production of privileged or work-product protected documents, ESI or information, whether inadvertent or otherwise, is not a waiver of the privilege or protection from discovery in this case or in any other federal or state proceeding. Nothing contained herein is intended to or shall serve to limit a party's right to conduct a review of documents, ESI or information (including metadata) for relevance, responsiveness and/or segregation of privileged and/or protected information before production. Inadvertent production of ESI later deemed privileged shall be governed by ¶ 12 of the Stipulated Protective Order filed separately.

29. **Time Zone.** The time zone used for a production shall be specified as required in Appendix A.

30. **Translations**. The producing party does not have an obligation to create an English translation of a document for purposes of discovery or associate an existing English translation to a foreign language original, when the documents are not located together or otherwise associated with one another in the ordinary course.

31. **Modification**. This Stipulated Order may be modified by a Stipulated Order of the parties or by the Court for good cause shown.

Dated: June 24, 2022

WHITE & CASE LLP

By: */s/ Bryan A. Merryman*

Bryan A. Merryman
(admitted *pro hac vice*)
WHITE & CASE LLP
555 South Flower Street
Suite 2700
Los Angeles, CA 90071
bmerryman@whitecase.com

Kathryn J. Mims
WHITE & CASE LLP
701 Thirteenth Street, NW
Washington, DC 20005
T: (202) 626-3704
F: (202) 639-9355
kmims@whitecase.com

Geoffrey W. Castello
KELLEY DRYE & WARREN LLP
One Jefferson Road, 2nd Floor
Parsippany, NJ 07054
Tel: (973) 503-5922
Fax: (973) 503-5950
gcastello@kelleydrye.com

Attorneys for Defendant
Gerber Products Company

Dated: June 24, 2022

COHEN MILSTEIN SELLERS & TOLL, PLLC

By: */s/ Steven J. Toll*

Steven J. Toll
COHEN MILSTEIN SELLERS & TOLL, PLLC
1100 New York Ave. NW
East Tower, 5th Floor
Washington, DC 20005
Telephone: (202) 408-4600
Facsimile: (202) 408-4699

Rosemary M. Rivas
GIBBS LAW GROUP LLP
1111 Broadway, Suite 2100
Oakland, CA 94607
Telephone: 510-350-9700
Facsimile: 510-350-9701

Janine Pollack
CALCATERRA POLLACK LLP
1140 Avenue of the Americas, 9th Floor
New York, New York 10036
Telephone: 212-899-1765
Facsimile: 332-206-2073

Plaintiffs' Interim Co-Lead Counsel

PURSUANT TO STIPULATION, IT IS SO ORDERED

Dated: _____

_____
Honorable Michael S. Nachmanoff
United States District Judge

APPENDIX A

Field Name	Description
PRODBEGBATES	The beginning bates number of a document
PRODENDBATES	The ending bates number of a document
PRODBEGATTACH	The first bates number in the attachment range of a document family
PRODENDATTACH	The last bates number in the attachment range of a document family
CONFIDENTIALITY	The confidentiality stamp for a document
PAGE COUNT	The total number of pages for the document
MD5 HASH	128 bit 32-digit hexadecimal number used to identify duplicates during file processing
FILETYPE	The type of file the document is
FILE EXTENSION	The file extension of the document
HAS COMMENTS/TRACK CHANGES	A Yes/No field identifying comments and track changes in Microsoft office documents
ALL CUSTODIANS	The custodian(s) or location(s) the data was collected from
ORIGINAL FILENAME	The name of the file
ORIGINAL FILEPATH	The path the file was stored in the normal course of business
DOC AUTHOR	The windows profile name attributed to the document
TO	The email addresses or names in the “TO” field
FROM	The email addresses or names in the “FROM” field
CC	The email addresses or names in the “CC” field
BCC	The email addresses or names in the “BCC” field
EMAIL SUBJECT	The subject line of the email
PARENT DATE (SORT DATE)	Date populated by the Sent or Received Date of an email and applied to its family members
SENT DATE	The date an email was sent
SENT TIME	The time an email was sent
RECEIVED DATE	The date an email was received
RECEIVED TIME	The time an email was received
CREATED DATE	The file system date stamp containing the original date a file was created
CREATED TIME	The file system time stamp containing the original time a file was created
LAST MODIFIED DATE	The file system date stamp containing the date a file was last modified
LAST MODIFIED TIME	The file system time stamp containing the time a file was last modified
REDACTED	A Yes/No field indicating whether the document contains redactions

TIME ZONE	The time zone which was used to process a file
TEXTPATH	The relative path to the document's extracted text / OCR file
NATIVELINK	The relative path to the document's native file, if applicable.